Brought to you by

CISCO

Phishing

for dummies®

A Wiley Brand

Cisco Special Edition

Build security resilience

Find the best technology to protect your organization

Defend against phishing attacks

Gabrielle Bridgers
Christina Hausman
Adam Tomeo
Ganesh Vellala Umapathy

Phishing

Cisco Special Edition

by Gabrielle Bridgers, Christina Hausman, Adam Tomeo, and Ganesh Vellala Umapathy

for dummies®
A Wiley Brand

Phishing For Dummies®, Cisco Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-21952-0 (pbk); ISBN 978-1-394-21953-7 (ebk)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Jen Bingham
Acquisitions Editor: Traci Martin
Editorial Manager: Rev Mengle
Sales Manager/other role: Molly Daugherty
Content Refinement Specialist: Tamilmani Varadharaj

Table of Contents

Introduction

All users are vulnerable to phishing. This is because phishing exploits aspects of human nature, such as our propensity to trust others or to be curious or to respond emotionally rather than rationally to alarmist messages. We may simply be too busy to spot anything suspicious in a phishing message. And when it comes to the more sophisticated attacks, it can be incredibly hard to spot a fake website or malicious message without special training.

Ultimately, phishing is effective because humans are fallible. This is where technology can help. Organizations should ensure that their cyberdefenses are up to the task of minimizing successful attacks and preventing phishing links from getting through to their people in the first place. When deployed effectively, cybersecurity can be a business enabler because it minimizes the risk of disruptions or financial loss.

About This Book

This book is intended to help you build resilience into your organization to properly defend it against phishing attacks. We look at how phishing has evolved in recent years, what new threats have emerged, and key social, political, and technological trends affecting the way attackers operate. We also look at some of the weaknesses in infrastructure, training, and protocols that leave organizations exposed to attacks and how to mitigate these weaknesses to stay ahead of the phishing threat. Finally, we look at specific Cisco solutions built to combat phishing and see how they work together to provide a strong defense against even the most sophisticated attacks.

Icons Used in This Book

Check the margins of this book and you'll observe some icons, which are guideposts to key points:

This isn't a lengthy novel, but if you're short on time and need to skim, don't miss the paragraphs marked with this icon.

The whole idea here is to learn something you can act upon, and the Tip icon points to a helpful bit of advice.

Warnings serve as practical guidance to help you steer clear of potential pitfalls, costly errors, or frustrating missteps, akin to the advice your mother might have given you.

There's much to consider when protecting your company from phishing attacks, and the Technical Stuff icon points to something you should know that goes a little more in depth.

Case studies about organizations dealing with phishing attacks.

Beyond the Book

It is impossible to convey in these pages all the ways in which Cisco's security solutions keep you protected from phishing attacks. You will find a range of free resources on their website that will help you get to know more about Cisco Secure Access, Umbrella, Duo, Secure Endpoint, Secure Email Threat Defense, and Cisco XDR.

You can also request a demo of any of their solutions or sign up for a free trial at `https://www.cisco.com/site/us/en/products/security/trials-offers.html`.

If you would like to discuss your organization's specific security needs and how Cisco can help you meet them, you're more than welcome to reach out to a Cisco representative near you. Details are available on their website at `https://www.cisco.com/go/security`.

IN THIS CHAPTER

- Defining phishing
- Examining attack types
- Seeing how attacks develop
- Understanding why phishing happens

Chapter 1
Phishing 101

Modern innovations like smartphones, cloud computing, and social media have given rise to a hyperconnected society and radically transformed the workplace. It has never been easier to keep in touch with your peers around the globe, expand your professional networks, or collaborate with your colleagues. The traditional office-based work model looks increasingly outdated today; with a plethora of digital communication channels and online tools at their fingertips, today's teams can work on complex projects without being in the same location.

However, there are downsides to this high level of digitization. One of the biggest is the fact that it has opened a host of new avenues for cybercriminals to carry out phishing attacks. These attacks can occur anytime and anywhere. Anyone who uses the Internet is vulnerable to them. This chapter introduces you to phishing and goes over some of the basics of phishing including the issues that lead to phishing attacks.

What Is Phishing?

Phishing is a type of electronically delivered social engineering attack in which a perpetrator, often posing as a legitimate entity, attempts to obtain sensitive information from an unsuspecting

individual or to infect their device with malware. The motivations for phishing attacks vary widely, but often attackers are after valuable user data, such as personally identifiable information or login credentials that can be used to commit fraud or access the victim's finances. In some cases, they may be trying to steal research, financial data, or health records from an institution. Some attackers may use phishing for social or political gain, as part of a hacktivism campaign, or to cause disruption or spread disinformation.

Though the practice of phishing is almost as old as the Internet itself, attacks have grown more sophisticated in recent years. It's not just about email anymore. Multistage, multivector attacks, bypassing traditionally secure multifactor authentication (MFA), have become the norm, and artificial intelligence (AI) chatbots are being used to craft increasingly error-free messages that are more effective in duping recipients into doing what the attacker wants.

Since the goal of these attacks is usually to trick Internet users into sharing credentials or following a malicious call-to-action (CTA), the consequences of falling prey to an attack can be dire. An IBM report released last year found that phishing was the second-most common cause of a data breach (accounting for 16 percent of breaches) as well as the costliest, leading to USD 4.91 million in average breach costs for organizations.

More than ever before, organizations need to be vigilant about the phishing threat and ensure that they have the right tools in place to defend against it. Thankfully, defenses have evolved to keep pace with increasingly sophisticated attacks. Turn to Chapter 4 to see some of the solutions Cisco has built to detect, respond to, and mitigate phishing threats. For more information on why phishing is on the rise, see Chapter 2.

Types of Phishing Attacks

Broadly speaking, phishing attacks fall into two categories (see Figure 1-1):

- **Mass phishing:** This targets a large group of people with a generic message. The attacker may send out thousands or even millions of emails that are identical or similar in content

in order to cast a wide net and capture as many victims as possible.

- **Spear phishing:** This is a targeted attack in which the attacker researches the victim and customizes the attack to make it appear more credible and convincing. The attacker may use information gathered from social media profiles, public records, or other sources to create a personalized message that appears to be from a trusted source, such as a colleague, boss, or friend, with the intent of tricking the victim into revealing sensitive information or performing a specific action, such as transferring funds or downloading malware.

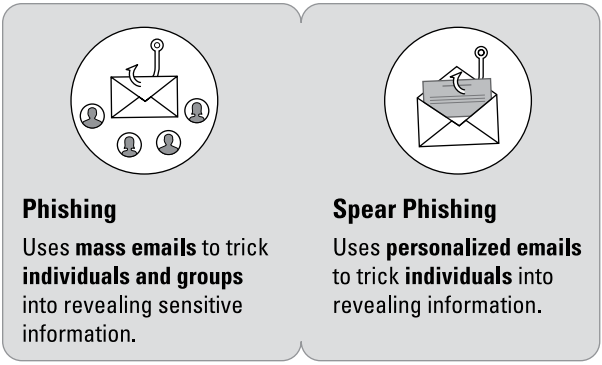

FIGURE 1-1: Spear phishing is customized to individuals whereas mass phishing doesn't have a particular target.

Additionally, phishing attacks can come through a variety of channels, including compromised websites, social media, fake ads, and text messages. While email is the most common attack vector, others include QR codes, workspace collaboration tools, and photo or audio attachments that may lead to advanced *steganography* attacks (hiding something malicious in a file that looks innocuous).

A more specific type of attack is called *typosquatting*, also known as URL hijacking, wherein an attacker registers domain names that are similar to well-known and frequently visited websites with the hope that users will accidentally mistype the legitimate website's address and land on their fake website instead. These fake websites might look almost identical to the real ones and can be used to phish for users' login credentials, credit card information, or other personal data.

Another example is an adversary-in-the-middle (AiTM) attack, also known as a man-in-the-middle (MiTM) attack, which involves the attacker intercepting communication between two parties to secretly eavesdrop, modify, or inject malicious code into the communication (see Figure 1-2). For instance, the attacker may intercept communication between the victim and a trusted organization, such as a bank or an online retailer, and then uses this information to impersonate the organization and trick the victim into providing sensitive information such as login credentials or credit card numbers.

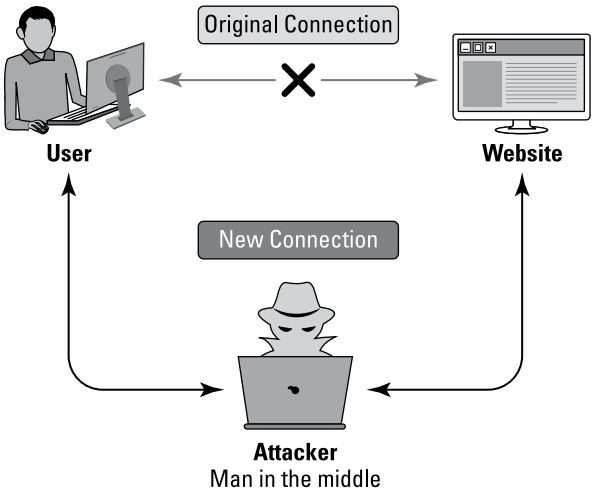

FIGURE 1-2: The attacker intercepts communication to cause trouble.

MEDIA COMPANY SPEARPHISHING ATTACK

CASE STUDY

In 2023, a media company that we'll call Company X experienced a highly targeted attack in which login credentials were obtained by the attackers.

The attackers sent convincing prompts to the company's employees, directing them to a website posing as Company X's intranet portal. This allowed them to steal login credentials and two-factor authentication tokens that gave them access to internal systems.

As a result, the attackers were able to steal internal documents containing employee data, including current and former employees' contact information, as well as bits of the source code for the company's news and community platform and information concerning advertisers.

Despite the significant loss of data, the attack was detected early due to the vigilance of a single employee who alerted security specialists that a data breach may have occurred. Company X acted swiftly, shutting down the cybercriminals' access and launching an internal investigation. The company also put its users on extra alert for attacks, and while no end-user data was stolen, they recommended that all users set up two-factor authentication on their accounts and use a password manager.

The Phishing Attack Process

A typical phishing attack involves getting the victim to click on a malicious link or weaponized file delivered by email, whereupon the victim's device will become infected with malware, or the victim will be directed to a clone of a trusted website and prompted to enter their login credentials. However, there are several other tactics attackers may employ.

Typically, these attacks take the following order:

1. **Reconnaissance:** Stalk potential victims on social media to discover vulnerabilities (for instance, find out where they work, where they live, what interests they have, and so on).
2. **Weaponization:** Craft an attack plan based on vulnerabilities from information gathered.
3. **Delivery of attack:** Send fraudulent emails, social media messages, or text messages based on vulnerabilities. These can contain malicious links or attachments and often alarmist content to drive a sense of urgency.
4. **Exploitation:** Steal credentials and personal information via fake portals that the victims were directed to.
5. **Monetization:** Access the victims' financial assets with harvested credentials then sell, siphon, or ransom off stolen data or assets. This is what drives many attackers to go to the trouble of setting up an attack.

Examining What Leads to Phishing Attacks

Many organizations today are putting themselves at heightened risk of falling victim to a phishing attack by not taking adequate measures to prepare. The following sections discuss some of the main gaps that leave organizations exposed.

Insufficient and ineffective cybersecurity infrastructure investments

Many organizations rely on cybersecurity defenses that are unable to cope with newer, more sophisticated threats. A recent Neustar International Security Council survey found that 49 percent of security decision makers felt that their organization's cybersecurity budget was insufficient to fully address their requirements, and 11 percent felt that they could only protect mission-critical assets.

Often the amount of money spent isn't the problem — it's the way money is spent. A survey of attendees at the 2022 RSA Conference found that 53 percent of the responding businesses feel they have wasted more than 50 percent of their cybersecurity budget and still can't remediate threats.

Gaps in personnel training

Often organizations neglect to provide their employees with the proper training to recognize the signs of potential risks, leaving them open to being tricked by phishing messages that look like legitimate business correspondence (see Figure 1-3 for an example).


TIP

Staff must transition from being responsive to being proactive in security. This requires training to spot phishing content that preys on personal narratives and current events. It is everyone's job to remain vigilant and keep sensitive information secure. By providing comprehensive training that keeps staff up to date with the latest threats and teaches them how to recognize them, organizations can help ensure the safety and security of their data.

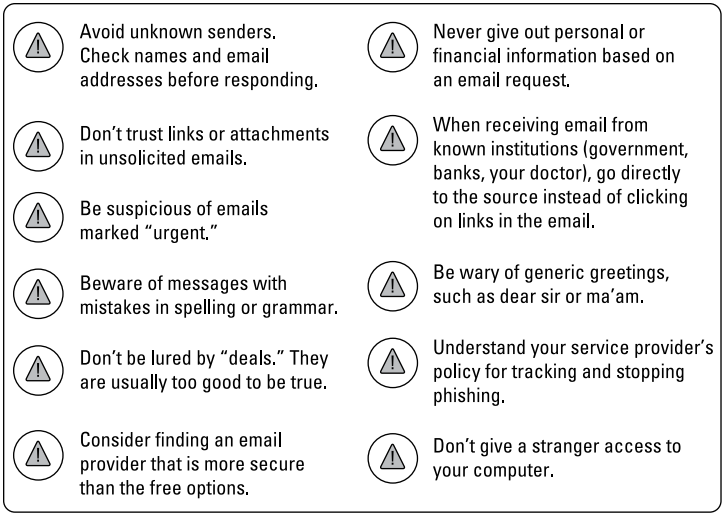

FIGURE 1-3: An example of good advice to protect against phishing.

A lack of security visibility

An increase in encrypted network traffic has led to a decrease in visibility for enterprise IT administrators, making it difficult to monitor both internal and external network activities. This lack of visibility poses a significant challenge for cybersecurity teams, because it limits their capability to protect systems, applications, identities, and workloads from advanced threats. Traditional security solutions often operate in silos, focusing on specific areas such as network security, endpoint protection, or cloud security. This siloed approach limits the visibility and context needed to detect and respond to sophisticated and coordinated attacks that traverse multiple vectors.

In the 2022 Security Visibility Report, released jointly by Cybersecurity Insiders and Cisco, it was found that the biggest challenge faced by cybersecurity teams is identifying which vulnerabilities pose a real threat and which ones are unlikely to be exploited by malicious actors. This concern was cited by 41 percent of survey respondents. Additionally, insufficient visibility into encrypted network traffic was also cited as a major obstacle, with 38 percent of respondents expressing concern.

According to Cisco's Security Visibility Report, the most significant gaps in network visibility were found to be in workload traffic, with 54 percent of respondents indicating a lack of visibility, followed by Software-as-a-Service apps (45 percent), network-connected devices (42 percent), and encrypted traffic (35 percent).

IN THIS CHAPTER

- Examining why phishing is increasingly common
- Looking at recent information about phishing

Chapter 2
The Evolving Phishing Landscape

The stakes of falling prey to a phishing attack are higher today than in the past because vast quantities of sensitive data are now stored in the cloud. Many organizations are ramping up digital transformation initiatives in order to streamline processes and more effectively use their data, and this often involves a greater dependence on cloud computing. In fact, McKinsey estimates that large enterprises aim to have about 60 percent of their environment in the cloud by 2025.

This chapter discusses the reasons that phishing is more prevalent today than it was in the past and goes over some recent insight into the world of phishing.

The Rise of Phishing

There is no doubt that cloud computing brings many benefits. McKinsey estimates that its adoption by organizations could generate USD 3 trillion in value worldwide by 2030 due to its capability to deliver operational cost savings, generate additional revenue

through things like advanced data analytics, and more. Without the cloud, organizations would not have been able to transition so easily to remote and hybrid work models during the pandemic.

REMEMBER

However, these benefits come with a significant cost — increased exposure to cyberattacks, including phishing. It's no coincidence that the increase in the amount of data stored on the cloud in recent years has been accompanied by a surge in data breaches. According to a white paper by Stuart E. Madnick, the number of data breaches more than tripled worldwide between 2013 and 2021. The situation is unlikely to improve — a Pricewaterhouse-Coopers study found that 38 percent of senior executives expect more serious attacks via the cloud in 2023.

Moreover, organizations are still heavily reliant on email, one of the top vectors for phishing attacks. According to Cisco, 1 in every 99 emails is a phishing attack, and 30 percent of those are opened. This doesn't even address the messages sent through social media or collaboration platforms.

Research has shown that phishing attacks increased dramatically during the COVID-19 pandemic. Since March 2020, 81 percent of organizations around the world have seen an increase in email phishing attacks. Additionally, data from Google Safe Browsing shows that there are now nearly 75 times as many phishing sites as there are malware sites on the Internet.

These facts make it clear that the phishing threat isn't going away any time soon. Indeed, the World Economic Forum has ranked "widespread cybercrime and cyber insecurity" as the eighth most severe global risk over the short term (two years) and long term (ten years). Since phishing attacks account for a large proportion of all cyberattacks, organizations cannot afford to ignore them.

New Insights into Phishing

Much research has been conducted on the subject of phishing, and on cybercrime more generally, over the years. The following sections discuss some of the key findings in recent studies.

Security needs to evolve to keep pace with the latest threats

Past phishing attacks focused on email as the primary delivery method. Phishing attacks also evolved using compromised or malicious websites and collaboration applications. This shows that attackers continue to evolve their attack methods based on how defenders respond to their current methods

It is widely understood now that password-based security isn't enough to protect against modern cyberattacks. The good news is that passwordless authentication is on the rise. The adoption of multifactor authentication (MFA) has increased around the globe. As part of this trend, the number of authentications using Cisco Duo rose 41 percent last year. On the other hand, biometrics enabled on mobile phones stalled at 81 percent last year after a steady increase over the last several years.

Web apps and email are key attack vectors

Despite the dizzying variety of digital communication tools on the market today, email use remains widespread around the world. Lifewire reports that a majority (62.86 percent) of business professionals prefer email to communicate for business purposes. According to Hotspot, there are 4 billion daily email users currently, and marketers continue to target them, with 77 percent reporting an increase in email engagement last year.

It's no surprise then that email continues to be a major attack vector for cybercriminals alongside web applications. According to Verizon's 2023 Data Breach Investigations Report (DBIR), web applications and email are the top two vectors for data breaches, accounting for over 60 percent and over 20 percent, respectively.

Cyberattacks continue to grow in complexity

Cybercriminals are growing increasingly innovative in the methods they employ to dupe people and circumvent cybersecurity defenses. For example, attackers are now using automated text-to-speech systems and audio deepfakes to conduct voice phishing, or *vishing,* attacks.

Additionally, attackers build org charts by scraping LinkedIn and other data stores. They collect mobile numbers for key individuals to automate imposter scams and send targeted text messages with phishing messages. This is called *SMishing* or text message phishing.

WARNING

Moreover, malware kits available on the dark web enable criminals with little to no coding skills to carry out highly sophisticated cyberattacks.

The malware economy mimics legitimate business. Hacking as a business has existed for many years. You can buy malware from one vendor and then pay another vendor to execute a phishing campaign for you. In its 2022 Global Risks Report, the WEF notes, "Sophisticated cyber tools are also allowing cyberthreat actors to attack targets of choice more efficiently, rather than settling for targets of opportunity, highlighting the potential to carry out more goal-oriented attacks that could lead to even higher financial, societal and reputational damage in the future."

CASE STUDY

WATCH OUT FOR "GREATNESS"

Almost anything these days can be offered as-a-service, so perhaps it's no surprise that phishing-as-a-service (PaaS) exists. A previously unreported PaaS offering named "Greatness" has been used in several phishing campaigns since at least mid-2022. Greatness incorporates features seen in some of the most advanced PaaS offerings, such as multifactor authentication (MFA) bypass, IP filtering, and integration with Telegram bots.

Greatness, for now, is only focused on Microsoft 365 phishing pages, providing its affiliates with an attachment and link builder that creates highly convincing decoy and login pages. It contains features such as having the victim's email address prefilled and displaying their appropriate company logo and background image, extracted from the target organization's real Microsoft 365 login page. This makes Greatness particularly well suited for phishing business users.

An analysis of the domains targeted in several ongoing and past campaigns revealed the victims were almost exclusively companies in the U.S., U.K., Australia, South Africa, and Canada, and the most commonly targeted sectors were manufacturing, health care, and

technology. The exact distribution of victims in each country and sector varies slightly between campaigns.

To use Greatness, affiliates must deploy and configure a provided phishing kit with an API key that allows even unskilled threat actors to easily take advantage of the service's more advanced features. The phishing kit and API work as a proxy to the Microsoft 365 authentication system, performing a "man-in-the-middle" attack and stealing the victim's authentication credentials or cookies.

Greatness is designed to compromise Microsoft 365 users and can make phishing pages especially convincing and effective against businesses.

Monitoring is insufficient

Organizations around the world spent around USD 150 billion on cybersecurity in 2021, reflecting an annual growth rate of 12.4 percent, according to a report from McKinsey & Company. Despite that expansion in investment, it may be insufficient considering the magnitude of the problem. Threat volumes are increasing substantially — nearly 80 percent of the observed threat groups operating in 2021, and more than 40 percent of the observed malware had never been seen previously.

REMEMBER

Organizations had problems defending against cyberattacks back when everyone was in the office and all applications and data were on-premises. The attack surface has increased exponentially with new business models, remote and mobile work, IOT, and cloud and hybrid environments. Defenders can't keep up. And the trend of buying new tools has created operational efficiency problems for defenders. Having to deal with multiple management consoles and stand-alone products from multiple vendors increases the difficulty.

Hiscox found that 58 percent of firms that qualify as cyberexperts consider their exposure to cyberattacks high or very high.

Humans can be the weakest link

Unfortunately, the human element can be a source of security pain. This is particularly true in regard to phishing, which is designed to prey on users' weaknesses. According to Verizon's 2023 Data Breach Investigation Report, "74 percent of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials, or social engineering." The report also states that Business Email Compromise attacks have almost doubled since 2022 and represent over half of all social engineering incidents.

IN THIS CHAPTER

- Implementing resilience
- Taking steps toward resilience
- Examining endpoints

Chapter 3
Building Resilience into Your System

To be better prepared for cyberattacks and phishing, organizations need to begin by building security resilience. In other words, they need to take a holistic approach to cybersecurity instead of pursuing piecemeal initiatives. Resilience is something all organizations should develop as a foundation to defend against phishing. This chapter discusses how you can build resilience to protect the integrity of every aspect of your organization so it can withstand unpredictable threats and emerge stronger.

Creating Security Resilience

Resilience requires the capability to manage any kind of change, whether positive or negative. This is because resilience provides confidence and certainty that threats can be met head-on anytime, anywhere — and successfully countered.

Steps toward resilience

So, how do you get started in building resilience? The most successful organizations tend to take the following steps (sourced from Cisco's research):

- **Foster a culture of security.** Employees should be made aware of the crucial role they play in keeping their organization safe from cyberattacks. They should be encouraged to report phishing attempts, potential malware, and other incidents. Establish accountability across all levels of business through security awareness training to improve cybervigilance and maintain compliance. Organizations that foster a culture of security see a 46 percent increase in resilience.
- **Identify your weaknesses.** Carry out an audit of systems, processes, technologies, and so on to uncover any weak areas that could potentially be exploited by a cybercriminal. Know your external risk from third parties, ensure that systems have no single points of failure, and prioritize using risk-based context analysis and continuous trust assessment of everyone and everything.
- **Develop executive-level representation.** Security resilience isn't just the security team's problem. There needs to be buy-in from the top levels of leadership. Organizations that report poor support from top executives show security resilience scores that are 39 percent lower than those with strong backing from the C-suite.
- **Have your resources in place.** Having surplus internal staff and resources on hand in order to better respond to unexpected cyberevents can improve an organization's resilience by 15 percent. If this isn't feasible for your organization, consider partnering with an external incident response service provider. Doing so could result in an 11 percent improvement in security resilience.
- **Implement a "security-by-design" mentality.** Establish strict security protocols and ensure that they're followed by all stakeholders. Don't wait for a breach to happen — develop an incident response plan as soon as possible.
- **Utilize threat intelligence as part of your detection and response capabilities.** Good cyberthreat intelligence helps organizations improve their detection and response capabilities by helping them know what to look for and how

to find it. Implement automated real-time continuous monitoring of endpoints.

- **Focus on simple-to-manage, flexible technologies.** When it comes to cybersecurity technology, simplicity is key, whether you're using on-premises or cloud environments. For example, multifactor authentication (MFA) can boost resilience by 11 percent and is generally simple to roll out and manage.
- **Implement layered security everywhere.** This includes implementing MFA for users, using endpoint detection and response (EDR) for endpoint security, securing email, protecting web traffic and cloud-based applications, and safeguarding the data they generate. Comprehensive visibility and control for all business resources must be ensured across on-premises, cloud, and multicloud environments. It is also essential to have visibility and control for employees, contractors, and third-party business partners.

Questions to answer

A focus on resilience has supercharged security concerns, raising difficult questions for today's executives:

- When will threats hit us?
- Are we prepared to detect all of them?
- Where are we most exposed to risk?
- Can we mitigate effects quickly?
- How fast can we recover?
- Are we getting better?

Putting Resilience into Action

There are three main aspects to security resilience, as we discuss in the following sections.

Prevention

To reduce the risk of ransomware attacks infecting systems, organizations should limit access to resources by requiring MFA for remote access to networks. Strong spam filters can also be enabled to prevent phishing emails from reaching end users, and

a user training program that includes simulated spearphishing attacks can be implemented. Additionally, filtering network traffic can prevent users from accessing malicious websites using URL blocklists and allowlists.


TIP

Regularly update software — including operating systems, applications, and firmware on IT network assets — in a timely manner. Using a centralized patch management system can simplify this process. Regular scans of IT network assets by antivirus/antimalware programs can help identify the presence of malware, and measures to prevent the unauthorized installation of software should also be put in place.

Containment

In the event of a cyberattack, responses to contain the attack are crucial. One such response is to isolate the infected system and remove its networking capabilities. In addition, infected and potentially infected devices should be collected and secured in a central location. It is also important to secure backups offline and scan backup data with an antivirus program to check for malware. Encrypted files can be recovered by specialists.


TIP

Implement segmentation at the workload and network levels to reduce the attack surface. If you have already segmented your network and key applications when a phishing attack penetrates your defenses, you will be able to identify it quickly and mitigate it before key information is stolen. That is proactive containment versus reactive.

Test and practice

Regularly testing contingency plans, such as manual controls, is crucial to ensure that safety-critical functions can be maintained during a cyberincident.

Features of a Resilient Endpoint

Endpoint security is critical to your organization's defenses. You can't protect everything from the network, and your endpoint protection solutions need to be able to collaborate and share context with the rest of your security defenses. There is a different viewpoint whether your solution is in the cloud, network, or on the endpoint. You must have all three, and the information must

be correlated between all solutions. The important thing is to ensure that all security solutions are fully integrated and working together to ward off attacks.

REMEMBER

It can be argued that the endpoint is where the most vulnerable section of any system tends to be. Protection here is fundamental to building resilience against phishing in both your security infrastructure and your people. One of the best ways to secure endpoints is to deploy endpoint detection and response (EDR) technology. However, not all EDR solutions are created equal. The most effective ones can do the following:

- Reduce dwell time to detect, remediate, and minimize impact fast
- Query the endpoint with any question and get answers in real time
- Proactively identify threats with built-in threat hunting
- Determine indicators of compromise (IoCs) through MITRE ATT&CK mapping
- Minimize noise from false positives

WORK SMARTER, NOT HARDER

While the phishing threat is not to be taken lightly, organizations have numerous tools at their disposal to combat it.

These days you don't need to be a security expert to ensure that your organization is protected from phishing threats, nor do you need to have a large security budget. When deployed effectively, technologies like AI allow security teams with limited budgets to implement robust defenses with minimal need for human intervention.

Another easy way to cut down on phishing is to develop an email-naming convention that doesn't follow the standard first.last name or first initial name pattern. This can help protect employees' email addresses from scammers, because randomizing email names across the organization will make employee email addresses difficult to guess on a mass scale. That way, a malicious email addressed to `joe.smith@yourcompany.com` will not find its way into Joe Smith's email account, protecting him from having to spend time deciding if it's legitimate or not and protecting your company from a possible intrusion.

IN THIS CHAPTER

- Introducing Cisco Secure Access
- Examining Umbrella and Secure Endpoint
- Highlighting Duo and Secure Email Threat Defense
- Getting to know XDR

Chapter 4
Cisco Products That Can Help Prevent Phishing Attacks

Effective security infrastructure is greater than the sum of its parts. It is only when tools, systems, and people work in tandem that an organization can be fully prepared to handle whatever threats come its way.

Cisco seeks to help you build a resilient organization that protects against even the most sophisticated phishing attacks. This chapter gives you an overview of the industry-leading solutions Cisco provides and explains how they work seamlessly together.

Cisco Secure Access

Today's challenging security reality, including pervasive and pernicious phishing, requires a smarter way to manage connectivity from anything to anywhere from everywhere, while simultaneously protecting against savvy, sophisticated attackers.

Security service edge (SSE) is an architectural approach that is designed to tackle cybersecurity risk in hyper-decentralized, hybrid work environments. It delivers secure access, comprehensive cloud-delivered security services, and centralized management for better protection against threats.

Cisco Secure Access is an SSE solution that helps end users securely access whatever they need to do their best work from anywhere. With extensive security capabilities converged in one solution, Cisco Secure Access mitigates security risk by applying zero trust principles and enforcing granular security policies. These capabilities include zero trust network access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), DNS security, remote browser isolation (RBI), and more.

Here are some of the core benefits Cisco Secure Access brings to the table:

- **Better for users:** Delivers seamless, frictionless connections to any application via any port or protocol, with optimized performance and continuous verification and granting of trust
- **Easier for IT:** Leverages a single, cloud-managed console to enable hybrid work through a simplified policy creation process, increased visibility, and aggregated reporting
- **Safer for everyone:** Tightens security and control by enabling DevOps to build security from the start and empowering SecOps to enforce zero trust principles across your distributed environment

What makes Cisco Secure Access unique? Here are a few examples:

- **A pragmatic ZTNA journey:** A new ZTNA architecture solves the challenges of last-generation ZTNA vendors, who don't support all application architectures such as multichannel applications, peer-to-peer applications, or server-initiated communication.

  By combining this next generation ZTNA with a fallback VPN-as-a-service (VPNaaS) in a single secure client, Cisco Secure Access transparently delivers a secure connection for all applications. End users can easily access the Internet, SaaS, or private applications — with no hassle and no friction.

- **Digital experience monitoring:** Cisco Secure Access incorporates ThousandEyes functionality to uniquely enable both end users and the IT helpdesk to resolve issues quickly by translating insights into proactive actions that optimize performance.
- **Part of the Cisco Security Cloud:** Cisco Secure Access is part of the Cisco Security Cloud, providing a comprehensive cloud-based management platform — with identity, posture, unified policy, design system, and service level agreement. This enables better protection against threats while making it easier to realize the combined benefits from across the Cisco portfolio and major third-party solutions.

Cisco Secure Access is an SSE solution that streamlines and simplifies secure connectivity and optimizes performance and security at every connection. It provides vastly better user experiences that drive worker productivity and simpler, cost-effective security operations to delight IT teams.

Umbrella

Cisco Umbrella offers flexible, cloud-delivered security that combines multiple security functions into one solution, all managed by a single console that integrates with Cisco network and security products. Umbrella allows you to extend data protection to devices, remote users, and distributed locations anywhere and can be set up in 30 minutes or less. It's a flexible tool with many use cases (see Figure 4-1).

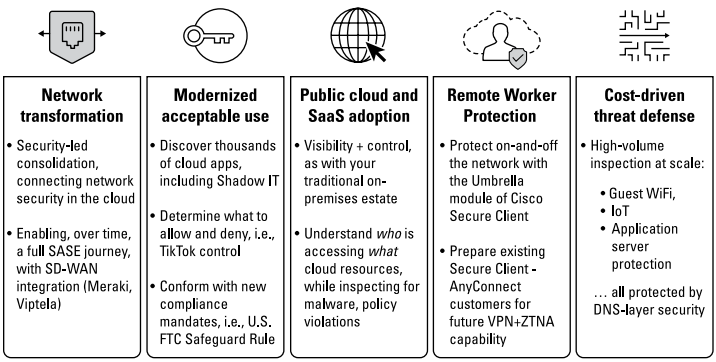

FIGURE 4-1: Core Umbrella use cases.

Umbrella enables unified threat management, bringing together secure web gateway, cloud-delivered firewall, cloud access security broker (CASB), and data loss prevention (DLP) functionalities. It also offers domain name server (DNS)-layer security and interactive threat intelligence in a single, integrated cloud service. This level of integration allows Cisco to provide comprehensive protection for distributed networks and roaming users.

When phishing is detected, Cisco Umbrella will block it at the IP and domain level as well as analyze risky domains in the DNS Intelligent Proxy, proactively preventing browser connections to risky websites. Every day, 50 million phishing attempts are tracked and blocked by Cisco Umbrella.

Modern cybersecurity with Secure Access Service Edge (SASE) capability

Organizations using Umbrella can simplify, secure, and scale with Secure Access Service Edge (SASE), a flexible architecture built specifically for hybrid workplaces, distributed networks, and companies with remote workers.

Cisco's SASE solution is comprised of Cisco SD-WAN and Umbrella. Branch internet access (DIA) is simplified with Cisco SD-WAN technology. As organizations shift their networking model to SD-WAN, security needs to remain top of mind. Branch offices and roaming users are more vulnerable to attacks, and as organizations move to more DIA, this becomes an even greater risk.

The Cisco SD-WAN and Umbrella integration enables you to infuse effective cloud security throughout your SD-WAN fabric so you can protect your branch offices and roaming users.

As opposed to traditional data center–oriented security, the SASE security model is placed at the cloud edge and offers security from end-to-end: the data center, remote offices, roaming users, and beyond. SASE provides secure access, whether an employee is logging into a cloud-based collaboration application or an on-premises application located inside the corporate data center.

The benefits of DNS-layer security

DNSs are at the heart of connecting every Internet request. Securing the DNS layer means blocking malicious domains, IP addresses,

and cloud applications before a connection is ever established. Umbrella blocks 170 million malicious DNS queries per day.

A solution that keeps up with evolving threats

Umbrella is always learning from new Internet events to prevent cyberattacks. Cisco Talos is a team of world-class engineers, mathematicians, and security researchers who build statistical and machine-learning models to automatically score and classify all of its data to detect anomalies and uncover known and emerging threats. Every second, Umbrella acquires and learns from over 1 million malicious and nonmalicious Internet events.

Maximize your security investment

Forrester Consulting recently completed an independent cost-benefit analysis of Cisco Umbrella to determine the financial and operational benefits of existing Umbrella customers' investments.

This comprehensive study found that Umbrella customers realized the following benefits:

- An impressive return on investment (ROI) after only three years
- A large decrease in the effort to deploy and enforce web and cloud security policies
- Security efficacy improvement
- Data breach reduction
- Increased security resilience

Secure Endpoint

Cisco Secure Endpoint is a single-agent solution that provides comprehensive endpoint detection and response (EDR) services and user access coverage to defend against threats to your endpoints, which leverages multiple approaches such as machine learning, behavioral analysis, file reputation, exploit prevention, and more. Cisco stops threats and blocks malware and then rapidly detects, contains, and remediates advanced threats that evade frontline defenses.

Secure Endpoint helps you stay resilient against attacks by helping organizations not only stop threats but also recover more quickly from attacks. After all, even with the best defenses, preventing every breach isn't possible. In these cases, it's critical to have a recovery plan and to strengthen your security posture.

Secure Endpoint is fueled by the breadth and depth of Cisco's portfolio, which protects 300,000 security customers worldwide. It also provides unique network insights because Cisco runs 80 percent of the world's Internet traffic.

Secure Endpoint has a strong track record of helping customers:

- Decrease their time to investigate and remediate threats
- Reduce the risk of a material breach and productivity loss
- Get more unique insights into threats across endpoints
- Simplify detection, response, and threat hunting
- Easily take immediate action on threats

CASE STUDY

MANUFACTURING COMPANY RANSOMWARE ATTACK

In the summer of 2020, a manufacturing company received a phishing email containing a malicious attachment. After an employee opened the email, several suspicious activities occurred. In the week that followed, the company received a notification from Cisco Talos Threat Hunting warning about this activity.

Cisco Talos Incident Response (CTIR) provided emergency response services, including incident command, expert guidance on containment and remediation, forensic analysis, threat intelligence, and reverse-engineering. CTIR began reviewing data from the Secure Endpoint, SecureX Cloud Edge, and Secure Network Analytics consoles, as well as triage data from affected hosts.

CTIR and Talos concluded that the activity Cisco Talos Threat Hunting alerted on was likely the beginning stages of a Maze ransomware

attack. Now allegedly disbanded, Maze was one of the more notorious ransomware families of late, engaging in "big game hunting," or targeting prominent organizations for large ransoms. They innovated the practice of exfiltrating data prior to dropping their ransomware, and then threatening to release the stolen data as another lever to compel victims to pay the ransom.

Maze adversaries typically maintain a long dwell time on the victim network as they search for privileged accounts and sensitive information. CTIR assessed that the adversaries had indeed been on the network several weeks before CTIR was engaged. However, this dwell time provided an opportunity for CTIR to identify the threat actor and thwart the more destructive elements of the attack.

CTIR quickly delivered a plan of action (POA) to the customer the day they were engaged, containing a series of steps to take to prevent the adversary from accessing even more systems, exfiltrating data, and dropping their ransomware. These actions had an immediate effect on the adversary's ability to move laterally throughout the network.

CTIR worked with the customer to push Secure Endpoint throughout the network and ensure it was running in Protect mode. With their avenues for lateral movement restricted, the adversaries dropped the ransomware binary on all systems they had previously accessed. The adversaries dropped the malicious DLL file on 130 systems. However, with Secure Endpoint running in Protect mode, the file was successfully quarantined, and the ransomware component of the attack was prevented.

Meanwhile, Talos safely detonated the ransomware file in Secure Malware Analytics. From there, they obtained the ransom note that confirmed the analysts' assessment that this was, in fact, a Maze ransomware attack.

This engagement exemplifies how CTIR leverages Talos-wide resources, past experience, and their expertise to deliver quick identification of threats as well as recommendations for remediation. With an active customer, CTIR prevented one of the most dangerous ransomware threat actors from achieving their goal.

A multifaceted endpoint security solution

Protect your endpoints with the following capabilities:

- **Prevent:** Identify and stop threats before compromise. Reduce the attack surface with multifaceted prevention techniques, risk-based vulnerability management, and posture assessments.
- **Detect:** Proactively hunt for hidden threats, detect stealthy malware, perform advanced investigations with actionable global threat intelligence from the industry-recognized Cisco Talos threat research team, and run complex queries to gain unprecedented visibility into your endpoints.
- **Respond:** Engage a powerful toolset that is easily deployed to help identify infected endpoints and understand the scope of an attack. In addition to multiple prevention and detection capabilities, Secure Endpoint offers granular endpoint visibility and response tools to handle security breaches quickly and efficiently.

In addition, Secure MDR for Endpoint offers dedicated teams of elite Cisco security experts in global Security Operations Centers (SOCs) providing around-the-clock protection.

Maximize your ROI

The Forrester Total Economic Impact (TEI) study commissioned by Cisco found that customers who deployed Cisco Secure Endpoint achieved a return on investment of up to 287 percent and payback in less than six months while reducing the time to investigate and/or remediate threats by 50 percent.

Furthermore, Cisco Secure Endpoint ranks as a Strategic Leader in the AV-Comparatives Endpoint Prevention and Response Test, with the highest efficacy and lowest total cost of ownership (TCO) per agent at USD 587 over 5 years. This real-world test emulates multistage attacks through a series of tests like MITRE ATT&CK evaluations.

Duo

Anything that can be logged into over the Internet should be protected with more than a username and password. This is why Cisco Duo allows you to verify the identity of users with strong and phishing-resistant multifactor authentication (MFA) options and to check the security health of their devices before they connect to the applications you want them to access.

Get insight into your security posture

Duo is a cloud-based access management solution that is scalable and designed to address security threats before they become problematic. It offers a range of tools besides MFA (see Figure 4-2), including passwordless authentication, risk-based authentication, endpoint remediation, and secure single sign-on (SSO) capabilities, which are simple and effective. These tools can be quickly deployed to control access in any environment with minimal downtime, thus optimizing productivity.

FIGURE 4-2: Duo offers a number of security features.

Additionally, Duo offers insight into the security posture of corporate and personal devices used to connect to company applications and services.

The solution combines intuitive usability with advanced security features to protect against the latest attack methods. It provides a frictionless authentication experience, ensuring the security of the entire organization.

Over the last year, Duo has introduced more than 20 security-oriented innovations such as passwordless and risk-based authentication and improvements to SSO, all of which help users protect themselves against phishing attacks.

Keep attackers out with zero-trust security

For organizations of all sizes that need to protect sensitive data at scale, Duo is the user-friendly zero-trust security solution for all users, all devices, and all applications.

REMEMBER

Zero trust is the future of information security. It takes security beyond the corporate network perimeter, protecting your data at every access attempt, from any device, anywhere.

Duo delivers zero-trust protection by enabling you to do the following:

- **Verify user trust:** Ensure that users are who they say they are at every access attempt — and regularly reaffirm their trustworthiness.
- **Establish device trust:** See every device used to access your applications and continuously verify device health and security posture.
- **Enforce adaptive policies:** Assign granular and contextual access policies, limiting exposure of your information to as few users and devices as possible.
- **Secure access for every user:** Provide appropriate permissions for every user accessing any application — anytime and from anywhere.
- **Secure access to every application:** Reduce the risk of credential theft by enabling users to securely access their applications with a single username and password.

Secure Email Threat Defense

Organizations rely heavily on email to conduct their business. This is why it remains the primary attack vector in phishing operations.

Cisco Secure Email Threat Defense provides comprehensive protection against damaging and costly email threats that compromise an organization's brand and operations. Its advanced threat

detection capabilities uncover known, emerging, and targeted threats.

Secure Email Threat Defense leverages unique artificial intelligence and machine-learning models, including natural language processing, to identify malicious techniques used in attacks targeting your organization; derives unparalleled context for specific business risks; provides searchable threat telemetry; and categorizes threats to understand which parts of your organization are most vulnerable to attack. Superior threat intelligence from Talos provides broader and deeper threat data that informs better and faster decision making.

Powerful search capabilities provide quick access to message details that empower more informed responses. Remediating threats directly in Threat Response streamlines processes and saves valuable time.

REMEMBER

As an important part of a larger Extended Detection and Response (XDR) strategy, Secure Email Threat Defense defends against critical threats with industry-leading threat intelligence, advanced threat detection capabilities, and vital telemetry that inform strategic threat protection. In combination with numerous third-party integration partners and the larger Cisco Secure portfolio of products, this provides the visibility, efficiency, simplicity, and telemetry that empower your team with the confidence to act quickly.

Orchestrating workflows in Cisco XDR simplifies processes, reduces the burden on your team, and builds efficiencies so you can focus on more strategic initiatives.

In short, Secure Email Threat Defense provides expansive email security to protect your employees and organization, while empowering your security response.

With Email Threat Defense customers can:

- Get complete visibility to inbound, outbound, and internal messages
- Use an integrated dashboard for search, reporting, and tracking, including conversation view and message trajectory

- Enhance Microsoft 365 security in less than five minutes without changing the mail flow
- Detect and block threats with superior threat intelligence from Cisco Talos, one of the largest threat research and efficacy teams
- Leverage fast API-driven remediation of messages with malicious content

Cisco XDR

Cisco XDR is a cloud-native extended detection and response solution for security operations teams that detects, prioritizes, and remediates threats more efficiently to achieve security resilience. Integrating with the broad Cisco security portfolio and many third-party offerings, Cisco XDR is one of the most comprehensive solutions on the market today.

Designed by security operation center (SOC) practitioners for SOC practitioners, Cisco XDR simplifies security operations to help security analysts remain proactive and resilient against the most sophisticated threats. By aggregating and correlating data from multiple disparate sensor and detection technologies into a unified view, Cisco XDR enables faster, more simplified investigations, reduces false positives, and enhances threat detection and response through clear prioritization of alerts, providing the shortest path from detection to response.

The built-in automation and orchestration in Cisco XDR, as well as guided remediation recommendations, allows security analysts to automate repetitive tasks easily and mitigate threats in the most effective ways, freeing up time and resources to focus on other proactive security tasks.

Designed specifically for SOC efficiency and ease of use, the data-driven and quantifiable Cisco XDR approach allows SOC teams to define the critical and most impactful events within their environment and focus remediate strategies there first, strengthening an organization's overall security posture and ensuring security resilience.

Detect the most sophisticated threats

Cisco XDR offers a robust range of native and third-party integrations for the most effective and scalable XDR strategy, optimized for a multivector, multivendor stack. It goes beyond the endpoint alone to collect and correlate telemetry from email, cloud, network, and more, to provide visibility across the entire security stack and detection of today's most sophisticated threats. It integrates with the full Cisco security stack, along with a specific set of third-party products. Events are enriched with asset insights, providing comprehensive device, user, and cloud insights to help identify security gaps.

Cisco XDR leverages telemetry from on-prem networks as well as public and private clouds, to alert on threats seen on managed and unmanaged devices, as well as to confirm and provide added context to alerts across the enterprise. Network telemetry, including firewall detections, helps provide a better understanding of critical context when correlating events, including where attacks start or spread throughout the network.

REMEMBER

Detections are strengthened with Talos threat intelligence, so analysts gain an unrivaled collection of actionable information for known and emerging threats, which provides deeper context and awareness of real-world threat behavior to enhance overall detection efficacy.

By bringing together and meaningfully correlating multiple telemetry sources, Cisco XDR provides actionable detections of complex threats that may have otherwise been overlooked.

Act on what truly matters, faster

Equip your security teams with effective threat prioritization, streamlined investigations, and evidence-backed recommendations.

Cisco XDR provides unified context and progressive disclosure techniques to simplify and compress investigation time. SOC analysts can aggregate alerts, global intel, and local context to understand root cause and the full scope of impact and always be action ready. Simplified investigation workflows allow decisive action to be taken more quickly.

Utilizing a progressive disclosure approach, Cisco XDR provides SOC analysts with the information they need to address current tasks without inundating them with extraneous data, which can cause confusion and analysis paralysis. SOC analysts are given the information they need, allowing them to make rapid and effective decisions based on relevant information.

The patent-pending prioritization capabilities of Cisco XDR help SOC analysts focus on the alerts/events that pose the greatest threat and take the right action immediately. Prioritization of these high-fidelity alerts is based on multiple factors, including threat intel, MITRE mapping, and real-world breach data to determine the likelihood that a threat will cause serious damage.

Elevate productivity

XDR can help eliminate noise and ease the skill shortage with automation and orchestration capabilities to boost your security team's efficiency and resources for optimal value. It can rapidly remediate threats in the environment with enhanced automation and configuration orchestration using predefined playbooks. With Cisco XDR, SOC teams can leverage a range of prebuilt or customizable orchestration workbooks to help shut down threats and mitigate risk in just a few clicks.

Organizations can boost limited resources for maximum value by automating repetitive and time-consuming tasks and providing SOC teams with built-in best practices. Cisco XDR also provides guided response suggestions and recommendations to help SOC analysts take effective response actions when automation isn't suitable.

Through deep security infrastructure integrations, analysts can quickly push response actions across a broad range of security tools, including Cisco and key third-party vendor solutions. Organizations can now update native and third-party prevention and protection compensating controls to prevent future incidents that mimic past threats. SOC analysts can also hunt across disparate alert logs as new tactics and techniques are discovered and new indicators of compromise are learned, taking a proactive role in threat hunting.

Build resilience

Cisco XDR helps SOC teams get better every day — making it possible for continuous, quantifiable improvement of their security posture (see Figure 4-3). SOC analysts can remediate threats while also fortifying their security controls and closing any security gaps, ensuring that they can prevent similar attacks in the future.

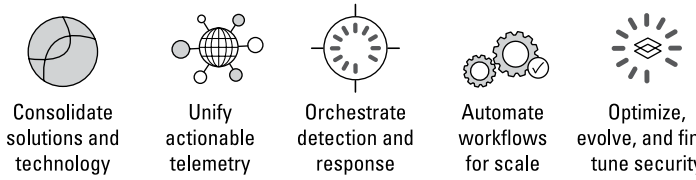

FIGURE 4-3: Cisco XDR positions your team to achieve incremental milestones.

Organizations can also start anticipating what's next. By tapping into actionable threat intel and expertise from Cisco Talos, Cisco XDR helps customers be better prepared for future threats.

Chapter 5
Five Key Phishing Trends

This chapter examines five emerging trends that will likely shape organizations' security responses for many years to come. These are not ranked in order of importance. Rather, each one is noteworthy in its own right.

AI Is a Game Changer

Artificial intelligence (AI) has been a gift to both phishing perpetrators and cybersecurity professionals. It has made it easier for attackers to carry out sophisticated, targeted, and more wide-scale attacks while also enabling advanced detection and prevention techniques.

WARNING

AI chatbots allow attackers to craft more convincing phishing messages free of spelling and grammar mistakes and to personalize these messages with data gleaned from the web. Attackers are also able to automate attacks by using bots to send out emails to large numbers of people.

According to the World Economic Forum, there are even concerns that machine-learning (ML) models could train themselves to carry out harmful and illicit cyberactivities.

On the other hand, AI can enhance cybersecurity defenses. For example, ML algorithms can be trained to identify phishing emails based on their content, sender, or other characteristics. This helps organizations to quickly identify and intercept phishing attempts before they can do any harm.

According to the International Data Corporation (IDC), AI in the cybersecurity market is growing at a compound annual growth rate of 23.6 percent and will reach a market value of USD 46.3 billion in 2027.

The Russia-Ukraine War Encourages New Threats

Ukraine has been defending itself from a variety of sophisticated cyberattacks since at least 2014, but Cisco Talos has observed an unprecedented number of adversaries clustered in the same threat landscape since the outbreak of the Russia-Ukraine war in February 2022. Ukraine's cybersecurity agency has claimed that it has witnessed a threefold increase in cyberattacks since the war began.

Various types of email lures related to the conflict, such as those with themes of humanitarian assistance and fundraising, have been sent by attackers. Although the primary intention of these emails is to carry out scams, they have also been used to deliver a range of threats, including remote access trojans (RATs), which are a type of malware that allows hackers to control machines remotely.

WARNING

Additionally, cybercriminals have been observed trying to exploit Ukrainian sympathizers by offering offensive cybertools to target Russian entities. In reality, these tools were malware.

Furthermore, state-sponsored attackers and other highly skilled adversaries have been extremely active during the war.

These cyberattacks are expected to continue even beyond the cessation of armed conflict in the future.

Log4j Exploitation Attempts Remain High

At the end of 2021, a critical security vulnerability was discovered in Log4j, a popular logging library for Java applications developed by the Apache Software Foundation. This library was widely used by numerous applications and programs, both commercial and open source.

WARNING

According to an article in *Wired*, cybercriminals are still exploiting the vulnerability, which has been dubbed Log4Shell, often using phishing techniques as the attack method to distribute malware and execute malicious code, even though patches have been released.

If an attacker exploits Log4Shell, they could completely take over an affected server. This is why the vulnerability has been assigned a Common Vulnerability Scoring System (CVSS) score of 10, which is the highest possible and indicates that it is a critical vulnerability.

Log4j is another example of a zero day attack. There have been many that have occurred in the past and they likely will continue in the future. Preparation is critical.

Politically Motivated Attacks Target Critical Infrastructure

Politically motivated cyberattacks are widespread today. *Hacktivism* (hacking for political purposes) has become more prevalent in recent years, with groups like Anonymous, LulzSec, and the Syrian Electronic Army gaining widespread attention for their high-profile attacks on government and corporate targets.

In addition, state-sponsored cyberattacks have proliferated in the context of the Russia-Ukraine war. Shortly before launching its invasion, Russia conducted a broad cybercampaign against Ukraine, with attacks focused on undermining critical sectors like energy, telecommunications, and financial services.

There has also been a rise in cyberattackers using ransomware to target critical infrastructure. For example, DarkSide, a cybercriminal organization believed to be behind the ransomware attack on Colonial Pipeline in 2021, is known to have developed ransomware-as-a-service and distributed it to affiliates.

While DarkSide has claimed to be apolitical, they have mainly targeted entities in Western nations and steered clear of the Commonwealth of Independent States, so it is fair to assume that their attacks are at least partly influenced by geopolitics. Moreover, there have been a number of ransomware attacks on governments in recent years.

There was a staggering 435 percent increase in ransomware in 2020, according to the 2022 Global Risks Report from the World Economic Forum (WEF). With this in mind, it is likely that ransomware will play a larger role in politically motivated cyberattacks around the globe over the coming years.

Newer Ways of Working Offer Attackers a Treasure-Trove of Data

Work from home (WFH) and hybrid work models allowed organizations around the world to continue operating throughout the various lockdowns imposed at the height of the COVID-19 pandemic. A host of collaboration platforms like Microsoft Teams, Google Workspace, Slack, and Webex helped to smooth the transition, providing a way for teams to carry out their responsibilities across multiple locations. Gartner reported that 80 percent of workers were using collaboration tools in 2021, an increase of 44 percent from the beginning of the pandemic.

WARNING

However, due to the vast amounts of data shared via these platforms, they have become an attractive target for cybercriminals. Forbes research found that a 50,000-person retail company sends more than 300 million collaboration messages each year, and an average of 1,500 shares of credit card information via Slack per month. Moreover, Veritas Technologies says that 71 percent of office workers globally have admitted to sharing sensitive and business-critical company data via instant messaging and business collaboration tools.

Strikingly, more than three out of five respondents to a 2022 Hiscox survey (62 percent) agree that their business is more vulnerable to attack with more employees working from home.

Email remains the primary attack vector in phishing, but security teams should definitely have collaboration tools on their watchlists.

Phishing attacks can happen anytime, anywhere

Modern innovations like smartphones, cloud computing, and social media have given rise to a hyperconnected society and radically transformed the workplace. However, these innovations have opened a host of new avenues for cybercriminals to carry out phishing attacks. This book discusses the ways in which phishing has become more prevalent and gives you pointers on how a resilient workplace can help you defend against it.

Inside...

- Types of phishing attacks
- Why phishing is increasingly common
- Taking steps toward resilience
- Cisco solutions that help fight phishing
- Key phishing trends

ISBN: 978-1-394-21952-0
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.